Introduction

The threat landscape progressively worsens by the day. Security teams spot ever-more sophisticated attacks in the wild and scramble to keep up. Faced with many new types of issues—including advanced phishing attacks that are all too successful and ransomware attacks many seem helpless to prevent—endpoint security strategies are evolving rapidly.

In the SANS “Endpoint Protection and Response” survey\(^1\) from 2018, 42 percent of respondents indicated at least one of their endpoints had been compromised, and 20 percent didn’t know if any endpoints had been compromised at all. Almost 20 percent found issues by proactively hunting, and more than 15 percent also stated they only discovered endpoint compromise via third-party notification. The last statistic tells the real story here: Many endpoint security tools and tactics in use today are inadequate, and we really need better prevention and detection tools right now.

Many attacks don’t leverage malware at all. Rather, savvy attackers may move laterally within network environments from host to host and use well-known system frameworks like PowerShell and other native Windows applications to avoid detection by tools that only look for “foreign” code and malware signatures. To add insult to injury, most agents—especially traditional antivirus tools—require a significant amount of agent overhead. This may not be reasonable for many hosts, especially those on legacy

systems with less powerful endpoints and already-overburdened servers. Many administrators are loath to install these kinds of tools if they can help it, but need something to ensure they meet compliance requirements.

Because of this failure of traditional endpoint security, organizations have begun adding more and more tools, leading to overwhelming complexity and not necessarily producing greater security. Most security analysts are barely able to keep up with all the disparate solutions we have in place, with too many agents and often disconnected teams trying to operate them. With the sophistication of attacks we see now, this creates a huge potential problem for enterprise teams trying to get ahead of sophisticated malware and attackers “living off the land” in attacks that don’t rely on malware at all.

Enter the CB Predictive Security Cloud platform. SANS had the opportunity to review the latest from Carbon Black, which now combines a lightweight, more behavioral-focused model of host-based protection with an integrated suite of powerful solutions for detecting, responding to and hunting for threats.

CB Predictive Security Cloud

The CB Predictive Security Cloud (PSC) seeks to provide a complete platform for securing endpoints to enable security teams to operate faster and more effectively. As its name implies, it relies on a cloud-based architecture and deployment model to deliver a swath of distinguishing key solutions that will be highlighted in this review.

For starters, the PSC has an extremely lightweight agent. The installation is small and fast regardless of the size of the organization involved, and once the agent is running, it adds negligible overhead to the endpoint in question. This last point is critical for operations teams that need to properly secure systems without adding so much overhead they effectively cripple performance.

Another key aspect of the PSC deployment is its cloud-based console. By putting the console in the cloud, Carbon Black consolidates what was once multiple separate consoles into one, and alleviates the operational burden of deploying an in-house management server. This makes deployment more flexible in mixed and hybrid environments where some systems are on-premise, while others are in various cloud environments like Amazon Web Services (AWS) or Microsoft Azure.

Third, the PSC benefits from a large intelligence-processing engine within the Carbon Black cloud, leveraging detection and prevention events spotted in the wild by agent deployments. Every Carbon Black customer benefits from the CB intelligence model, which benefits the entire community over time.

While we didn’t test this directly, it is also important to note that unlike closed, siloed solutions with islands of data that are difficult to integrate and extend, the PSC is built on open APIs. This makes it easy for other security vendors to deliver pre-built integrations and creates a network of integrated solutions to help customers increase visibility, efficiency and speed across their security ecosystem. Open APIs enable organizations to custom-build their security stack with integrated solutions to amplify
the investments they've made in Carbon Black and other security tools, and the resulting services easily extend and scale to support custom workflows as organizations grow and mature. The PSC platform integrates with many other cybersecurity tools and platforms, easily sharing critical endpoint data across the entire security stack for better detection and response workflows.

Finally, the PSC captures detailed forensic information about attempted and thwarted attacks, which allows defenders to examine evidence and learn from the attacks to better investigate and prepare for future incidents.

**Updated Platform**

Carbon Black updated its platform from the original endpoint technology seen in the SANS review of CB Defense in 2017 to a cohesive ecosystem of services that can interoperate and use a strong intelligence engine built on a scalable cloud platform. The key functionalities of the PSC include:

- **Next-generation antivirus (NGAV) and endpoint detection response (EDR)**—Carbon Black’s NGAV and EDR solution solves the challenges of security efficacy, visibility and operational effectiveness. These capabilities allow the PSC to stop both known and unknown attacks in real time.

- **Virtual data center security**—Thanks to the PSC’s ability to work in a software-defined infrastructure that offloads antimalware processing and VMware API-integrated monitoring and remediation, it protects internal virtual environments from malware as well. This was not tested during the SANS review.

- **Threat hunting and incident response (IR)**—The threat hunting and IR solution on the PSC delivers unfiltered visibility for top security operations centers (SOCs) and IR teams. These capabilities pull together endpoint data and threat intelligence to provide a customized visualization of attacks.

- **Real-time endpoint query and remediation**—Live query and response enables teams to ‘ask a question and get an answer’ of their entire fleet of endpoints. Powered by osquery, this feature enables a wide variety of use cases such as extended threat hunting, patch management and IT hygiene.

- **Managed alert triage**—The PSC’s managed threat alerting service provides threat validation and trend analysis by experts. This was not evaluated during the SANS review.

**CB Predictive Security Cloud: Ease-of-use and Integration**

The PSC review environment examined two scenarios. The first involved using some Windows virtual machines running in an online lab environment. These had the latest PSC agent installed and provided access to all platform capabilities. The second was based on a Kali Linux system for attacks and testing.

---

The online PSC console is simple to navigate. The main screen shows the recent detection events and activities and provides a number of informative graphs and charts that give us quick access to suspicious activity information, specific events that matched Kill Chain attack stages, attacks broken out by attack vectors and device/application breakouts (see Figure 1).

One of the dashboard elements we thought was particularly interesting was the “Potentially Suspicious Activity” listing, which included cases of suspicious executables or tools and services (think PowerShell) that may be exhibiting malware-like tendencies and could be suspicious in particular circumstances. We also explored the different ways we could configure the dashboard, which was simple with the “Configure Dashboard” function available on the main screen. We explored how we could use the PSC and its dashboard in different attack workflows, considering the platform within the context of three different—and sometimes overlapping—user cases for this review. The following scenarios served as a basis for our review of the core PSC components:

- **Security analyst**—Using the PSC as a security analyst who would be monitoring the environment within a SOC, we found the existing screens and graphs/charts to be perfectly suited to this task. A SOC analyst needs to immediately see attack phases detected, attacks stopped and suspicious activity.

- **Incident responder or threat hunter**—These security roles may also need the SOC analysts’ view of attacks and suspicious activity. The PSC lets organizations configure dashboards for basic breakdowns of devices and applications seen on protected endpoints.

- **Desktop admin**—Desktop admins care far less about attacks by vector or potentially suspicious activity, but want to focus on attacks stopped (which would let us determine whether an attack is related to an issue a user was experiencing), as well as endpoint health and top applications seen (and possibly top devices in some cases).

Overall, we found the dashboard view of the PSC to be highly configurable and very easy to use when looking for information and drilling down into it.
Antivirus and EDR Capabilities

The first major function of the PSC we reviewed was its NGAV and EDR capabilities, which serve as the PSC’s primary attack detection and prevention component. At the heart of this service lies the “Alerts” pane: Most users will spend quite a bit of time here looking at detected threats, including those that were prevented and blocked. Organizations would look for the following in an endpoint prevention and detection engine:

- An intuitive and easy-to-navigate interface when looking at what’s happening in the environment currently
- Quick access to specific types of threats, if desired
- Quick analysis of what the threat tried to do, if prevented, or where to look for follow-up activity if the threat could not be blocked for some reason

Easy-to-Configure Interface

The PSC meets all of these requirements. First, to get a sense of the types of threats seen in the environment, we clicked into the Alerts pane from the left-hand menu. We appreciated the simple breakdowns revealed by this navigational pane, which let us custom-configure the information on the main screen to focus only on top priority alerts. This, in turn, can help analysts easily hone-in on what they’re looking for amidst suspicious activity. For example, you could delimit activity by:

- **Type**—We could select CB Analytics (the big data analytics engine driving Carbon Black detection and prevention), Watchlists (specific items we instructed the PSC to watch for) or both.

- **Category**—Here we could select asset value ranges (defined and tagged within the product), alert severity or types of alerts, for example with labels such as “Threats” or simply “Monitored” (less severe). The “Target Value” label is a unique differentiator, and makes alerts and actions within the PSC much more contextual. Organizations should give high-value assets priority, and this asset value definition is a quick way to query important systems for analysts.

- **Devices**—Analysts can choose specific systems to monitor or show alerts for, as desired.

- **Applications**—We can select specific applications noted in alerts.

- **Workflow**—Analysts can dismiss unimportant or false positive alerts. Note that Alerts have a default setting of “Not Dismissed.” This pane allows us to show those Not Dismissed or Dismissed quickly.

You can also show alerts based on policy status, specific policies and specific tags that are customizable. Any alerts handled by an existing PSC policy are flagged with a red icon in the console as “Policy Applied.” See Figure 2.
In addition, the PSC has a highly flexible search capability built into the interface, which enabled us to quickly look for key terms like ransomware and PowerShell, or specific behaviors we may be interested in. This feature allows analysts to dig through large numbers of alerts rapidly to find only those of interest. For much more granular analysis of a specific alert event, we chose to dig into a high priority alert by clicking the Alert Triage button to the right of the specific event. This takes us into a detailed workflow breakdown that shows the entire execution flow of the attempted attack and includes information about the alert and system involved; policy actions taken; and processes, files and communications involved (see Figure 3).
Prevention and Quarantine

In our first attack scenario, we found the console identified a number of noteworthy elements for this alert:

- Outlook was used to open Excel (not that uncommon).
- Then Excel started PowerShell, which is highly suspect.
- PowerShell next attempted to communicate to a remote system, access a Microsoft executable (`conhost.exe`) and drop a file (which the PSC immediately shows us a hash value for).

In this scenario, we deliberately triggered this string of events in our test environment and then purposefully went into Windows Explorer to try and access the file that was dropped (`krrgbt.exe`). This action was denied per our policy, which illustrates the powerful “quarantine in place” method that the PSC uses. Rather than quarantining the files or removing/obfuscating them immediately, the PSC locks them away from everything on the system so they can’t cause harm. However, users can retrieve quarantined files for evidence and later investigation easily with the Take Actions button on the right (choose “Request Upload”).

Additional actions include automatic whitelisting or blacklisting of processes, files or IP addresses; and the ability to battle potential new malware by automatically submitting unknown binaries for dynamic analysis in a cloud sandbox. Another great feature is the Quarantine Device button on the right, a function of the PSC sensor that will take over the affected system’s network stack, prohibiting it from communicating to anything besides the PSC. In the bottom pane, we had much more specific details of what occurred in this alert (see Figure 4).

For the second malicious attack workflow we explored, we queried the Alerts main pane for ransomware in the filter box and then selected a high severity alert for Alert Triage as before. In this example, however, we have many more actions and files included in the attack execution and multiple attempts to start new PowerShell commands. These later PowerShell commands set a destination for encrypted files, then attempt to access files on the OS by abusing PowerShell’s access to `explorer.exe`, finally attempting...
encryption of these files—all of which are classic ransomware behaviors. Figure 5 illustrates the more advanced execution flow—the highlighted PowerShell attempt. The detail panel on the right shows specific techniques, tactics and procedures (TTPs) for this execution based on Carbon Black’s behavioral monitoring.

We also delved into the Alert Origin pane on the bottom, which concatenates all the behaviors seen within the alert context and generates a useful visualization map of the risks perceived by Carbon Black alongside the grouped TTPs (see Figure 6).

Our final exploration of alerts allowed us to see another PowerShell example, but this time the command accessed a batch file (*persistence.bat*) that adds a Windows scheduled task. In the current policy, this behavior is not explicitly disallowed, so we wanted to modify the policy in place to prevent this from happening in the future. Looking at the execution flow, we can see the whole thing begins with Excel opening PowerShell—which is a logical thing to stop entirely in order to prevent attacks like this happening at all. We clicked into the Enforce pane on the left, choosing Policies. In our Standard policy, we can easily add prevention steps that will prohibit this execution flow from here on out. To do this, we clicked Add application path at the bottom of the screen, add **\excel.exe** (anything matching this string pattern) in the applications path dialog box and then select the Deny operation policy that prevents Excel from invoking a command interpreter (See Figure 7).
Additionally, we can take this new policy element, copy it and push it out to all other policies or only select policies we choose. Overall, the policy engine has been significantly streamlined and enhanced within the PSC and we were impressed with how simple and flexible the process was to build powerful preventive and detective endpoint security policies and enable them on all endpoints. (The average policy heartbeat check-in across the entire organization is roughly five minutes.) Looking at the rest of the policy engine updates, we could see how analysts would love the ability to choose different policy update and scanning cycles as well. We chose an “aggressive” scan cycle (meaning both new and pre-existing files are immediately assessed against the Carbon Black malicious file library prior to execution) and regular signature updates. Signatures remain useful in catching known malware, and using local signatures allows the PSC to function as a direct antivirus replacement. See Figure 8.

Figure 7. Customizing PSC Module Policies

Figure 8. Scan Configuration
After working through several examples of nasty attacks and malware, we were impressed with the capabilities Carbon Black offered us. The PSC gave us the capability to rapidly detect malware, prevent many malicious activities at a granular level through policy and dig into deep forensic detail about what happened—or at least what the attackers attempted on endpoints. The search and filter capabilities within the Alerts pane was easy to use, and would allow any security analyst to quickly dig into the precise and relevant details needed to escalate the investigation or handle it appropriately.

**Threat Hunting**

For SOC analysts, IR teams and generally any threat hunting professionals, we need to dig into event data at a deeper level and move to a more proactive model of analysis within the environment. That’s where the PSC’s threat hunting and IR service comes in. With this service, we can query anything noted by the Carbon Black agent across the entire environment at a highly granular level.

In keeping with our first example—a phishing email causing dangerous process execution—we went to the Investigate tab and chose to look for anything that had Outlook as a parent investigation. This is easily done by entering a search query of 

```
parent_name:outlook.exe
```

in the query interface (see Figure 9).

We can tailor the query even more to look for file paths, groups of devices, usernames involved, parent process and other such items with the filters on the left-hand pane. For example, in phishing attacks it is common for Outlook to open a document attached to an email and subsequently launch in PowerShell. We used the example of Outlook as the parent, which then leads to Excel being opened and spawning PowerShell, and refined our PSC query to 

```
parent_name:outlook.exe AND childproc_name:powershell.exe
```

(The PSC also auto-fills query syntax to help you develop these and get moving more quickly.) See Figure 10 for a more precise query.
By clicking any of these more targeted results, we can see a very tailored and complete view of exactly what was spawned or attempted during an attack scenario, which would be much more useful information for a threat hunter or incident responder who needed to get highly detailed information. We can also add additional filters for things like Windows Registry changes, file changes, process changes and more (see Figure 11).

The detail pane at the bottom of Figure 11 shows us highly detailed entries for all behaviors associated with the selected process, in this case including native Windows file access, some of the malicious files we saw earlier (\krrgb.exe) and more. We next explored one of the more advanced capabilities, Live Response. We clicked the Go Live button within the PSC to open a live response shell on the affected host, giving us a specific set of capabilities to analyze the system as needed.

In this case, we chose to look for any scheduled tasks running (given the persistence script we saw in the last example). Figure 12 shows us running the `execfg` command to run PowerShell and check any Scheduled Tasks in place.
Note within the code the attacker has added a malicious persistence task called **thinkillstay** at the bottom of the figure. Back at the prompt, we can execute another command to remove that task, as shown in Figure 13.

As a final example of how the PSC’s threat hunting service can perform more efficient investigations and environment analysis, we went back to the earlier example where an Outlook query led to a PowerShell execution. In this case, we created a Watchlist for this to a PowerShell execution scenario by returning to the **Investigate** pane, then selecting the **Add query to watchlist** button on the far right of the query bar. See Figure 14 to see how we created a new watchlist that will alert us any time Outlook leads to a child PowerShell process.
The threat hunting component of the PSC can also leverage third-party threat intelligence feeds and information from partners of Carbon Black. Furthermore, it has a number of built-in watchlists.

Looking at the PSC from the perspective of a desktop analyst or someone more focused on “fixing the issues” in an environment, Carbon Black can really help to dig into what’s happening quickly by using the “Live Query” pane. This functionality is built on osquery from the team at Facebook, an open source project allowing SQL-like queries against endpoints to look for specific information and potential indicators of compromise. A key difference for Carbon Black is it shows us what is happening on systems right now versus what happened in the past. Carbon Black can also be used to query systems for insights even when there is no malicious or suspicious activity underway. For example, we could search for a specific browser plugin installed across all systems even if the plug-in was not an immediate cause for concern. In the context of the malicious workflows we examined in the NGAV and EDR components of the PSC during
this review, we could look for Scheduled Tasks with specific names (thinkillstay), files dropped (krrgbt.exe) and many additional specific items like Registry keys, service names and others. An example of the query to look for the Scheduled Task is shown in Figure 15, along with a successful response from a protected system.

Of note: Any remediation action (for example, deleting the scheduled task) can also be scripted through API access to remediate systems across all Carbon Black’s agent installs. In other words, we can rapidly fix any problems discovered as a result of queries returned. The Carbon Black User Exchange also includes a huge number of prebuilt queries ranging from administrative tasks to security operations that customers have contributed for use by others (see Figure 16).

Any of these queries can then be immediately brought to Carbon Black’s Live Query and pasted into the SQL Query pane to send to all systems. This is a powerful tool to help all analysts—including desktop and help desk teams—find problems in the environment and contribute to incident response and security investigations, as well as proactive hunting exercises.
Conclusion

The endpoint is a notoriously difficult asset to protect today. Laptops, workstations and servers are constantly under siege, and the traditional tools we've relied on are failing us more and more often. The CB Predictive Security Cloud platform offers a unique approach to prevention, detection and remediation in the enterprise, with a lightweight agent that is managed from the cloud and has deep introspection into behaviors and unusual activity (as opposed to solely relying on signature-based prevention and detection). The platform is also comprehensive in what it offers. It is a complete endpoint security replacement that could immediately benefit teams who need to consolidate tools instead of managing multiple endpoint agents and consoles. Furthermore, the PSC’s strength comes through in how it supports security operations teams: As teams work to become more proactive, the need to perform threat hunting and rapid investigation across large numbers of systems has become more urgent.

The SANS team found the PSC very easy to set up and use, and observed several scenarios in which the tool could prevent or detect and monitor at a very granular level. Most security teams need more specific data related to attack attempts today. The PSC offers not only powerful prevention capabilities, but also in-depth forensic, threat hunting and monitoring controls that teams can use to help prevent incidents throughout their environments. We found the platform can easily provide immediate value to information security analysts (for detection and analysis of malicious activity in the environment); to SOC analysts, incident responders, threat hunters (for deeply delving into forensic details of events occurring and tracking down compromised hosts); and to desktop admins (for diagnosing and resolving endpoint problems in a short amount of time).
About the Author

Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

SANS would like to thank this paper’s sponsor:

Carbon Black.